# Metric Structure of Linear Codes

Diego Ruano
ruano@mathematik.uni-kl.de - University of Kaiserslautern (Germany)

Complexity, Coding, and Communications. Institute for Mathematics and its Applications. April 16-20, 2007

## Toric Codes

Toric geometry studies varieties that contain an algebraic torus as a dense subset and furthermore the torus acts on the variety. The importance of these varieties, called toric varieties, is based on their correspondence with combinatorial objects, this makes the techniques to study the varieties more precise.

J.P. Hansen defined in 1998 the toric codes, algebraic geometry codes over a toric variety. A convex rational polytope is the same datum as a normal toric variety $X_P$ and a Cartier divisor $D_P$. For a polytope $P$ of dimension $r$ we obtain the **toric code** $\mathcal{C}_P$ by evaluating rational functions at the $(q-1)^r$ points of the algebraic torus $T \simeq (\mathbb{F}_q^*)^r$. $\mathcal{C}_P$ is the image of the linear evaluation map

$$\begin{array}{rcl} \mathrm{ev} : \mathcal{L}(D_P) & \to & (\mathbb{F}_q)^{\# T} \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

The dimension of the codes is computed using cohomology theory. The minimum distance is estimated using intersection theory or by a multivariate generalization of Vandermonde determinants.

---

Toric codes have been extended to

## Generalized Toric Codes

- $U \subset H = \{0, \ldots, q-2\} \times \ldots \times \{0, \ldots, q-2\}$, $T = (\mathbb{F}_q^*)^r$
- $\mathbb{F}_q[U] \subset \mathbb{F}_q[Y_1, \cdots, Y_r]$ the $\mathbb{F}_q$-algebra generated by

$$\{Y^u = Y_1^{u_1} \cdots Y_r^{u_r} \mid u = (u_1, \cdots, u_r) \in U\}$$

The **generalized toric code** $\mathcal{C}_U$ is the image of the $\mathbb{F}_q$-linear evaluation map

$$\begin{array}{rcl} \mathrm{ev} : \mathbb{F}_q[U] & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

- Generalized toric codes are $r$-D cyclic codes (or multicyclic codes).
- Their dual and their metric structure were computed and studied in [D. Ruano: *On the structure of generalized toric codes*, arXiv:cs.IT/0611010, 2006].
- In this new work we have studied the metric structure of linear codes and obtained similar results to those for generalized toric codes for an arbitrary linear code.

---

## Metric Structure of Linear Codes

- $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, $B(x, y) = \sum_{i=1}^n x_i y_i$ the bilinear form used to define the dual code of a linear code.
- $\mathbb{F}_q^n$ will be the vector space over $\mathbb{F}_q$ with the non-degenerated symmetric bilinear form $B$ whose associated matrix is the identity matrix.
- If $\mathbb{F}_q^n$ is the direct sum of mutually orthogonal spaces

$$\mathbb{F}_q^n = U_1 \oplus \cdots \oplus U_r$$

  then we say that $\mathbb{F}_q^n$ is the orthogonal sum of $U_1, \ldots, U_r$ and it is denoted by

$$\mathbb{F}_q^n = U_1 \perp \cdots \perp U_r$$

Let $H \subset \mathbb{F}_q^n$ be a two-dimensional vector subspace, it is said that $H$ is a **hyperbolic plane** if there exist $x_1$, $x_2$ such that they generate $H$ and

$$B(x_1, x_1) = 0, \; B(x_2, x_2) = 0, \; B(x_1, x_2) = 1$$

A non-singular two-dimensional vector subspace $E \subset \mathbb{F}_q^n$ is an **elliptic plane** if there exist $x_1, x_2$ which generate $E$ and such that

$$B(x_1, x_1) = 0, \; B(x_2, x_2) = 1, \; B(x_1, x_2) = 1$$

---

### Characteristic of $\mathbb{F}_q$ different from 2

- $\mathbb{F}_q^n$ has a **geometric decomposition of type** $r, s$ if

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s$$

  where $H_1, \ldots, H_r$ are hyperbolic planes and $L_1, \ldots, L_s$ are non isotropic one-dimensional linear varieties.
- Each hyperbolic plane is generated by two geometric generators $H_i = \langle x_{2i-1}, x_{2i} \rangle$, such that $B(x_{2i-1}, x_{2i-1}) = 0$, $B(x_{2i}, x_{2i}) = 0$, $B(x_{2i-1}, x_{2i}) = 1$, for $i = 1, \ldots, r$.
- Each one-dimensional variety is generated by $L_i = \langle x_{2r+i} \rangle$, for $i = 1, \ldots, s$.
- One has that $\{x_1, \ldots, x_n\}$ is a basis of $\mathbb{F}_q^n$ that we call **basis of the geometric decomposition**.

Let $M$ be the matrix of $B$ in the basis of the geometric decomposition, then one has that $MM^t = J_{r,s}$

$$J_{r,s} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \varepsilon_1 & & \\ & & & & & & \ddots & \\ & & & & & & & \varepsilon_s \end{pmatrix}$$

where $\varepsilon_i$ is either $1$ or a fixed non-square of $\mathbb{F}_q^*$.

A linear code is said to be **compatible with a geometric decomposition of type** $J_{r,s}$ if there exists a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ compatible with such a decomposition, in such a way that exists $I \subset \{1, \ldots, n\}$ such that $\{x_i \mid i \in I\}$ is a basis of the code.

**Theorem.** *Let the characteristic of $\mathbb{F}_q$ be different from 2. Any linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is compatible with at least one geometric decomposition of type $r, s$ with $s \leq 4$.*

---

### Characteristic of $\mathbb{F}_q$ equal to 2

- $\mathbb{F}_q^n$ has a **geometric decomposition of type** $r, s, t$ if

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s, \text{ with } t = 0$$

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s \perp E, \text{ with } t = 1$$

  where $H_1, \ldots, H_r$ are hyperbolic planes, $L_1, \ldots, L_s$ are isotropic one-dimensional linear varieties and $E$ is an elliptic plane
- Each hyperbolic plane is generated by two geometric generators $H_i = \langle x_{2i-1}, x_{2i} \rangle$, such that $B(x_{2i-1}, x_{2i-1}) = 0$, $B(x_{2i}, x_{2i}) = 0$, $B(x_{2i-1}, x_{2i}) = 1$, when $i = 1, \ldots, r$.
- Each one-dimensional variety is generated by $L_i = \langle x_{2r+i} \rangle$, such that $B(x_{2r+i}, x_{2r+i}) = 1$ when $i = 1, \ldots, s$
- The elliptic plane is generated by two geometric generators $E = \langle x_{n-1}, x_n \rangle$ if $t = 1$, such that $B(x_{n-1}, x_{n-1}) = 0$, $B(x_n, x_n) = 1$, $B(x_{n-1}, x_n) = 1$.
- One has that $\{x_1, \ldots, x_n\}$ is a basis of $\mathbb{F}_q^n$ which we call **basis of the geometric decomposition**.

Let $M$ be the matrix of $B$ in this basis, then one has that $MM^t = J_{r,s,t}$

$$J_{r,s,0} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

$$J_{r,s,1} = \begin{pmatrix} 0 & 1 & & & & & & & & \\ 1 & 0 & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & 0 & 1 & & & & & \\ & & & 1 & 0 & & & & & \\ & & & & & 1 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & 1 & & \\ & & & & & & & & 0 & 1 \\ & & & & & & & & 1 & 1 \end{pmatrix}$$

A linear code is said to be **compatible with a geometric decomposition of type** $J_{r,s,t}$ if there exists a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ compatible with such a decomposition, in such a way that exists $I \subset \{1, \ldots, n\}$ such that $\{x_i \mid i \in I\}$ is a basis of the code.

**Theorem.** *Let $\mathbb{F}_q$ with characteristic 2. Any linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is compatible with at least one geometric decomposition of type $r, s, t$ with $s \leq 4$ and $t = 0$ or $s = 0$ and $t = 1$ ($s = 0, t = 1$ is only considered for self-dual codes).*

---

Let $\{x_1, \ldots, x_n\}$ be a geometric basis of a geometric decomposition of type $r, s, t$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Let $i \in I$, we define $i'$ as

- $i + 1$ if $x_i$ is the first generator of a hyperbolic plane $H$
- $i - 1$ if $x_i$ is the second generator of a hyperbolic plane $H$
- $i$ if $x_i$ generates a linear space $L$
- $i + 1$ if $x_i$ is the first generator of an elliptic plane $E$
- We do not need to define $i'$ when $x_i$ is the second geometric generator of an elliptic plane

For $I \subset \{1, \ldots, n\}$ we define $I' = \{i' \mid i \in I\}$, $I^\perp = \{1, \ldots, n\} \setminus I'$.

**Proposition** *Let $\mathcal{C}$ be a linear code with a geometric decomposition of type $r, s, t$ given by the basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$. Let $I \subset \{1, \ldots, n\}$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Then the dual code $\mathcal{C}$ is $\mathcal{C}^\perp = \langle x_i \mid i \in I^\perp \rangle$.*

- $M$ the $n \times n$-matrix whose rows are the elements of the basis $\{x_1, \ldots, x_n\}$, then $MM^t = J_{r,s,t}$.
- $M(I)$ the $k \times n$-matrix consisting of the $k$ rows with $i \in I$, then $M(I)$ is a generator matrix of $\mathcal{C}$.
- $M(I^\perp)$ is a control matrix of $\mathcal{C}$, that is, $M(I^\perp)$ is a generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$.

---

### Orthogonal Group and Linear Codes

- $\mathcal{M}_{r,s,t} = \{M \in \mathcal{M}_{n \times n} \mid MM^t = J_{r,s,t}\}$ with $(s, t) \in \{0, 1, 2, 3, 4\} \times \{0\} \cup \{0\} \times \{1\}$ and $2r = n - s - 2t$, allows us to define the family of linear codes throughout their submatrices.
- Reciprocally, any subset of rows of a matrix of this type can be considered as a generator matrix of a linear code.
- The orthogonal group acts over $\mathcal{M}_{r,s,t}$.
- We have obtained a new paradigm for linear codes.

**Acknowledgements:** Partially supported by DASMOD-Cluster of Excellence in Rhineland-Palatinate (Germany) and MEC MTM2004-00958 (Spanish Ministry of Education and Science).